PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-172638
(43)Date of publication of application : 23.06.2000

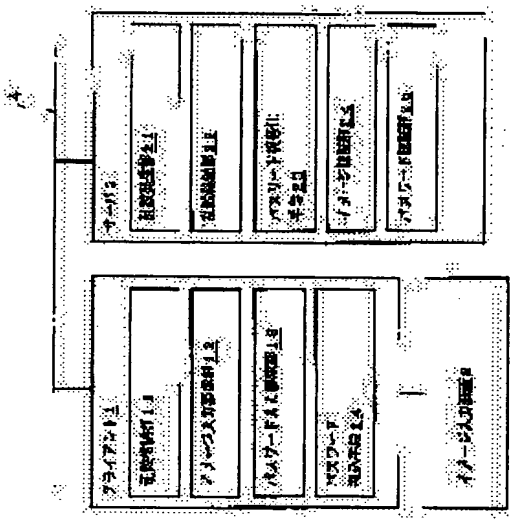
(51)Int.Cl. G06F 15/00
G09C 5/00
H04L 9/32

(21)Application number : 10-346862
(22)Date of filing : 07.12.1998

(71)Applicant : NEC CORP
(72)Inventor : FUJIZU HISAYUKI

(54) TRANSMISSION AND RECEPTION DATA CERTIFYING SYSTEM

(57)Abstract:
PROBLEM TO BE SOLVED: To improve reliability in electrically interception prevention of data to be electrically intercepted of for which electrical interception is not desired.
SOLUTION: This system is provided with a password imbedding means 14 for embedding a password, for which wire tapping on a network 4 is not wanted, into an image, password decoding means 23 for extracting the password embedded by the password embedding means 14 from the image, password certifying part 24 for certifying the password decoded by the password decoding means 23, and image certifying part 24 for certifying the image, based on the password certified by the password certifying part 24.



LEGAL STATUS

[Date of request for examination] 17.03.1999
[Date of sending the examiner's decision of rejection] 26.02.2002
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－172638
（P2000－172638A）
(43)公開日　平成12年６月23日(2000.6.23)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｇ０６Ｆ　15/00	３１０	Ｇ０６Ｆ　15/00	３１０Ｂ	５Ｂ０８５
Ｇ０９Ｃ　5/00		Ｇ０９Ｃ　5/00		５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ａ	９Ａ００１
			６７３Ｄ	

審査請求　有　　請求項の数４　ＯＬ　（全４頁）

(21)出願番号　特願平10－346862

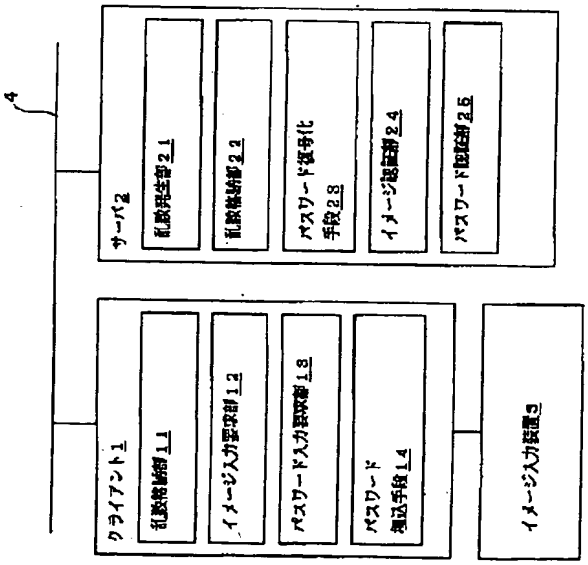
(22)出願日　平成10年12月７日(1998.12.7)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　藤津　久行
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100089875
弁理士　野田　茂

Ｆターム(参考)　5B085 AE03 AE09 AE23 BG07
5J104 AA01 AA08 AA16 EA16 LA02 NA05 PA07
9A001 CC02 EE02 EE04 GZ22 JJ12 JJ27 LL01 LL03

(54)【発明の名称】　送受信データ認証方式

(57)【要約】
【課題】　送受信される盗聴されたくないデータの盗聴防止についての信頼性を向上させること。
【解決手段】　ネットワーク４上で盗聴されたくないパスワードをイメージに埋め込むパスワード埋込手段１４と、該パスワード埋込手段１４により埋め込まれた前記パスワードを前記イメージから抽出するパスワード復号化手段２３と、該パスワード復号化手段２３により復号した前記パスワードを認証するパスワード認証部２４と、該パスワード認証部２４により認証したパスワードをもとに前記イメージについての認証を行うイメージ認証部２４とを備える。



1

【特許請求の範囲】

【請求項１】　送受信するデータについての認証を行う送受信データ認証方式において、

前記データをイメージに埋め込むデータ埋込手段と、

該データ埋込手段により埋め込まれた前記データを前記イメージから抽出する復号化手段と、

該復号化手段により復号した前記データを認証する認証手段と、

該認証手段により認証したデータをもとに前記イメージについての認証を行うイメージ認証手段と、

を備えたことを特徴とする送受信データ認証方式。

【請求項２】　乱数を発生する乱数発生手段を有し、前記データ埋込手段は、前記乱数発生手段により発生した乱数をもとに、データのイメージ上への埋込位置を決め、前記データをイメージに埋め込み、前記復号化手段は、前記乱数発生手段により発生した乱数をもとに、前記イメージ上の前記データの埋込位置を知り、前記データを前記イメージから抽出することを特徴とする請求項１記載の送受信データ認証方式。

【請求項３】　前記データ埋込手段は、前記乱数発生手段により発生した乱数をもとに決定されたイメージの画素位置にデータをＲＧＢデータに変換して埋め込み、前記復号化手段は、前記乱数発生手段により発生した乱数をもとに、前記イメージの前記画素位置に前記データが埋め込んであることを知り、ＲＧＢデータとして埋め込んである前記データを復号化することを特徴とする請求項２記載の送受信データ認証方式。

【請求項４】　前記データは、サーバとクライアントとの間で送受される印鑑やサイン等のイメージデータのパスワードであることを特徴とする請求項１乃至３に何れか１項記載の送受信データ認証方式。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、例えばサーバ、クライアント間において送受信されるデータの送受信データ認証方式に関し、特に盗聴されたくないデータをイメージに埋め込むことにより、当該データの盗聴を阻止する送受信データ認証方式に関する。

【０００２】

【従来の技術】従来、一般にネットワーク上で送受信されるデータの認証、例えば印鑑やサイン等のイメージデータの認証にはパスワードが使われているが、このパスワードはテキストデータでネットワーク上を流れる。

【０００３】

【発明が解決しようとする課題】従来の送受信データ認証方式は以上のようにパスワードにより行われており、テキストデータでパスワードがネットワーク上を流れるため、パスワードが簡単に盗聴でき、ネットワーク上の盗聴に対してはもろい課題があった。

【０００４】そこで本発明の目的は、送受信される盗聴されたくないデータの盗聴防止についての信頼性を向上させた送受信データ認証方式を提供することにある。

2

【０００５】

【課題を解決するための手段】本発明に係る送受信データ認証方式は、送受信するデータをイメージに埋め込むデータ埋込手段と、該データ埋込手段により埋め込まれた前記データを前記イメージから抽出する復号化手段と、該復号化手段により復号した前記データを認証する認証手段と、該認証手段により認証したデータをもとに前記イメージについての認証を行うイメージ認証手段とを備えたことを特徴とする。

【０００６】本発明の送受信データ認証方式は、送受信するデータをイメージに埋め込み、該埋め込まれた前記データを前記イメージから抽出して復号化し、該復号化した前記データを認証し、該認証したデータをもとに前記イメージについての認証を行い、特に前記送受信するデータをイメージに埋め込む際に、送信側および受信側共通の乱数により前記データの前記イメージへの埋込位置を決めることで、ネットワーク上で送受信される前記データの盗聴防止についての信頼性を向上させる。

【０００７】

【発明の実施の形態】以下、本発明の実施の一形態について説明する。本実施の形態の送受信データ認証方式は、サーバ、クライアントによる印鑑やサイン等のイメージデータの承認において、パスワードを前記イメージデータに埋め込むことによりパスワードの盗聴を阻止することで、ネットワーク上で送受信される前記印鑑やサイン等のイメージデータの盗聴や偽造などの防止についての信頼性を向上させるものである。

【０００８】またパスワードをイメージに埋め込む際に乱数を使用することにより埋め込み場所をその時々によって変えることにより、前記イメージデータを盗聴されてもパスワードの盗聴を不可能に出来るセキュリティ機能を有する送受信データ認証方式である。

【０００９】図１は、本実施の形態の送受信データ認証方式の構成を示すブロック図である。この送受信データ認証方式は、乱数格納部１１、イメージ入力要求部１２、パスワード入力要求部１３およびパスワード埋込手段（データ埋込手段）１４を備えたクライアント１と、イメージ入力装置３と、乱数発生部（乱数発生手段）２１、乱数格納部２２、パスワード復号化手段（復号化手段）２３、イメージ認証部（イメージ認証手段）２４およびパスワード認証部（認証手段）２５を備えたサーバ２と、クライアント１とサーバ２を接続するネットワーク４から構成される。

【００１０】クライアント１は、イメージ承認を要求するものである。サーバ２は、イメージ承認を行うものである。クライアント１の乱数格納部１１は、サーバ２より転送された乱数を格納するものである。イメージ入力要求部１２は、認証をする際にイメージの入力を促し読

み込むものである。パスワード入力要求部１３はイメージ入力後にパスワードの入力を促し、読み込むものである。パスワード埋込手段１４は、乱数格納部１１に格納されている乱数より演算を行い、イメージのどの場所にパスワードを埋め込むかを決定するものである。具体的な例としては、イメージの縦１００ピクセル、横５０ピクセルの位置にパスワードをＲＧＢデータに変換して埋め込むといった作業である。メージ入力装置３は実際のイメージを読み込む装置である。

【００１１】サーバ２の乱数発生部２１は乱数を発生するものである。乱数格納部２２は、乱数発生部２１が発生した乱数を格納するものである。パスワード復号化手段２３は、乱数格納部２２に格納されている乱数をもとに演算を行いイメージのどの場所にパスワードが埋め込んであるかをサーチし、パスワードをイメージから復号化するものである。具体的な例としは、イメージの縦１００ピクセル、横５０ピクセルの位置にパスワードが埋め込んであることをサーチし、ＲＧＢデータとして埋め込んであるパスワードを復号化するといった作業である。イメージ認証部２４は、クライアント１から認証要求のあったイメージを認証するものである。パスワード認証部２５は、クライアント１から認証要求のあったパスワードを認証するものである。

【００１２】図２は、本実施の形態の送受信データ認証方式の動作を示すフローチャートであり、同図（ａ）はサーバ側、同図（ｂ）はクライアント側の動作を示す。以下、これらフローチャートに従って動作を説明する。先ず、クライアント１から認証要求があると（ステップＳ１）、サーバ２において乱数発生部２１が乱数を発生させ、乱数格納部２２に乱数を格納する（ステップＳ２，ステップＳ３）。次に、サーバ２の乱数発生部２１で発生させた乱数をクライアント１に転送し（ステップＳ４）、クライアント１の乱数格納部１１に前記乱数を格納する（ステップＳ５，ステップＳ６）。その後、クライアント１のイメージ入力要求部１２が、認証に必要となるイメージ入力を促し、イメージ入力装置３を用いてイメージを取り込み、取り込んだイメージはイメージ入力要求部１２に格納される（ステップＳ７）。イメージを取り込み終えた後、パスワード入力要求部１３が認証に必要となるパスワード入力を促し、パスワードが入力されると、入力されたパスワードはパスワード入力要求部１３に格納される（ステップＳ８）。

【００１３】次に、パスワード埋込手段１４が、乱数格納部１１に格納されている乱数を取り出し、イメージ要求部１２からは格納されているイメージを、パスワード要求部１３からは格納されているパスワードを取り出し、パスワード埋込手段１４により取り出した乱数により演算を行い、イメージのどの部分にパスワードを格納するか決定し、パスワードをイメージデータに変換し、前記イメージにパスワードを埋め込む（ステップＳ９）。具体的な例としてはイメージの縦１００ピクセル、横５０ピクセルの位置にパスワードをＲＧＢデータに変換し埋め込む。

【００１４】その後、クライアント１はパスワードを埋め込んだイメージデータをサーバ２に転送する（ステップＳ１０）。サーバ２は、パスワードを埋め込んだイメージデータをクライアント１から受け取り、パスワード復号化手段２３に格納する（ステップＳ１１，ステップＳ１２）。

【００１５】次に、パスワード復号化手段２３は乱数格納部２２から乱数を取り出し、取り出した乱数で演算を行い、転送されてきたパスワードが埋め込まれたイメージデータのどの部分にパスワードが格納されているのかをサーチし、イメージデータとして格納されているパスワードを当該イメージデータから変換して取り出す（ステップＳ１３）。具体的な例としては縦１００ピクセル、横５０ピクセルの位置にＲＧＢデータとして埋め込まれたパスワードを変換し、通常のテキストデータに復号化する。

【００１６】最後に、イメージ認証部２４がイメージデータを認証し（ステップＳ１４）、パスワード認証部２５が復号化されたパスワードを認証し（ステップＳ１５）、全プロセスが終了する。

【００１７】従って、本実施の形態によれば、パスワードをイメージに埋め込んでいるため、サーバ２、クライアント１による印鑑やサイン等のパスワードを用いたイメージ承認においてパスワードの盗聴を高い信頼性で阻止できる。

【００１８】また、パスワードをイメージに埋め込む際に乱数を使用することにより埋め込み場所をその時々によって変えるため、イメージデータを盗聴された場合であっても、パスワードの盗聴防止については高い信頼性を確保できる。

【００１９】なお、印鑑やサイン等を用いたイメージ認証のみならず秘密データを送受信する際にイメージデータに秘密データを乱数を用いて埋め込むように構成してもよく、高いセキュリティ機能を確保できる。

【００２０】

【発明の効果】以上のように、本発明によれば、送受信するデータをイメージに埋め込み、該埋め込まれた前記データを前記イメージから抽出して復号化し、該復号化した前記データを認証し、該認証したデータをもとに前記イメージについての認証を行う構成を備えたので、ネットワーク上で送受信される盗聴されたくないデータの盗聴防止についての信頼性を向上できる効果がある。前記ネットワーク上で送受信するデータをイメージに埋め込む際に、送信側および受信側共通の乱数により前記データの前記イメージへの埋込位置を決める構成を備えるようにしたので、ネットワーク上で送受信される前記データの盗聴防止についての信頼性をより向上できる効果

5

がある。

【図面の簡単な説明】

【図１】本発明の実施の一形態の送受信データ認証方式の構成を示すブロック図である。

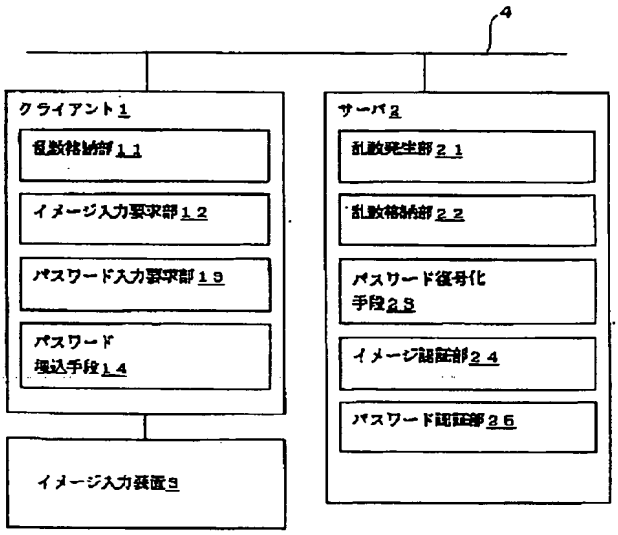
【図２】本発明の実施の一形態の送受信データ認証方式の動作を示すフローチャートである。

6

【符号の説明】

４……ネットワーク、１４……パスワード埋込手段（データ埋込手段）、２１……乱数発生部（乱数発生手段）、２３……パスワード復号化手段（復号化手段）、２４……イメージ認証部（イメージ認証手段）、２５……パスワード認証部（認証手段）。

【図１】



【図２】